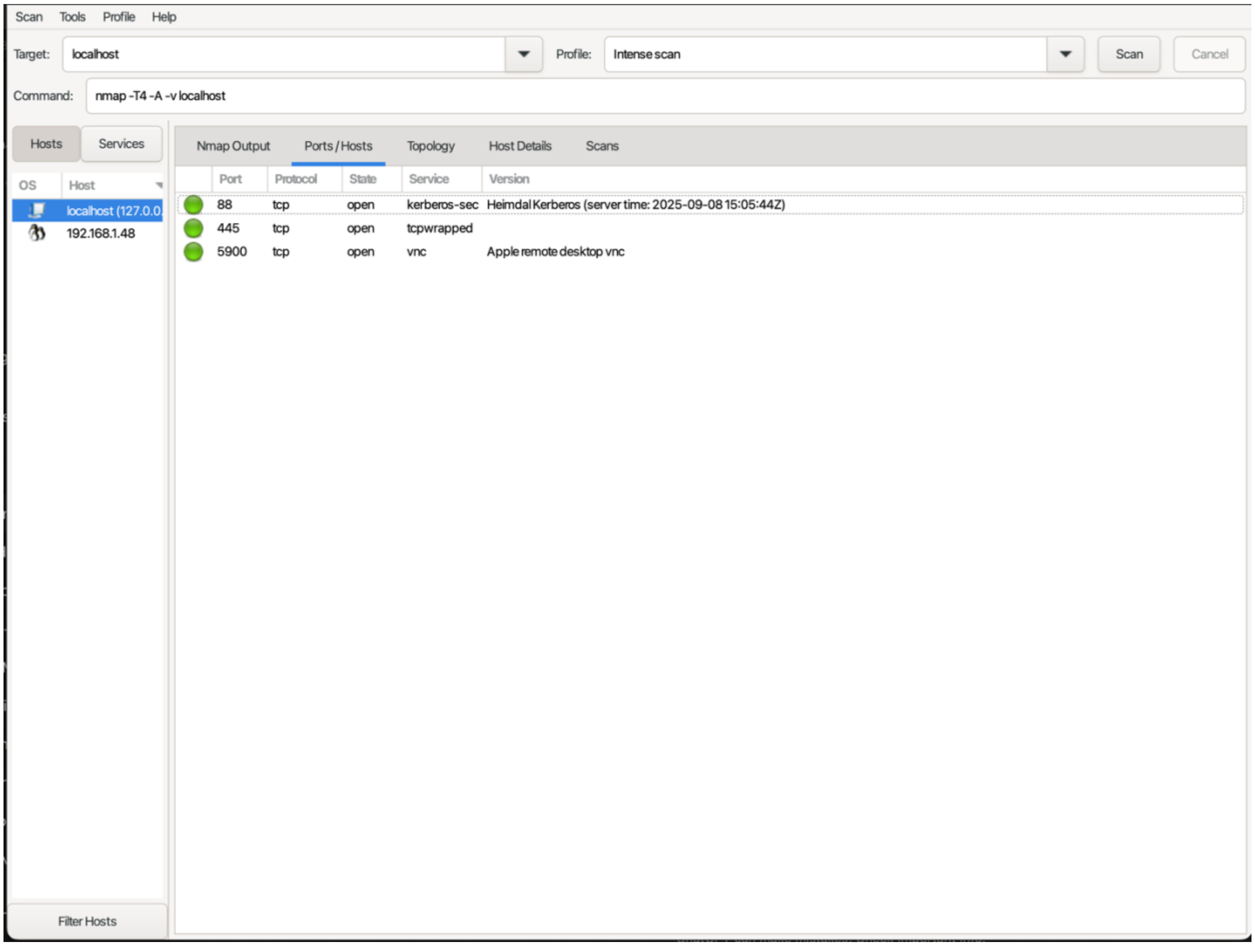
Chayanin Kongsareekul 6532035021

Activity 3

Q1.

Notice the open ports on all 3 devices (the attacker notebook, the target notebook, and the target Linux VM). Does anything look suspicious, i.e., some ports that you are not aware of that are open on the VM or on your notebooks?



Target: localhost

Profile: Intense scan

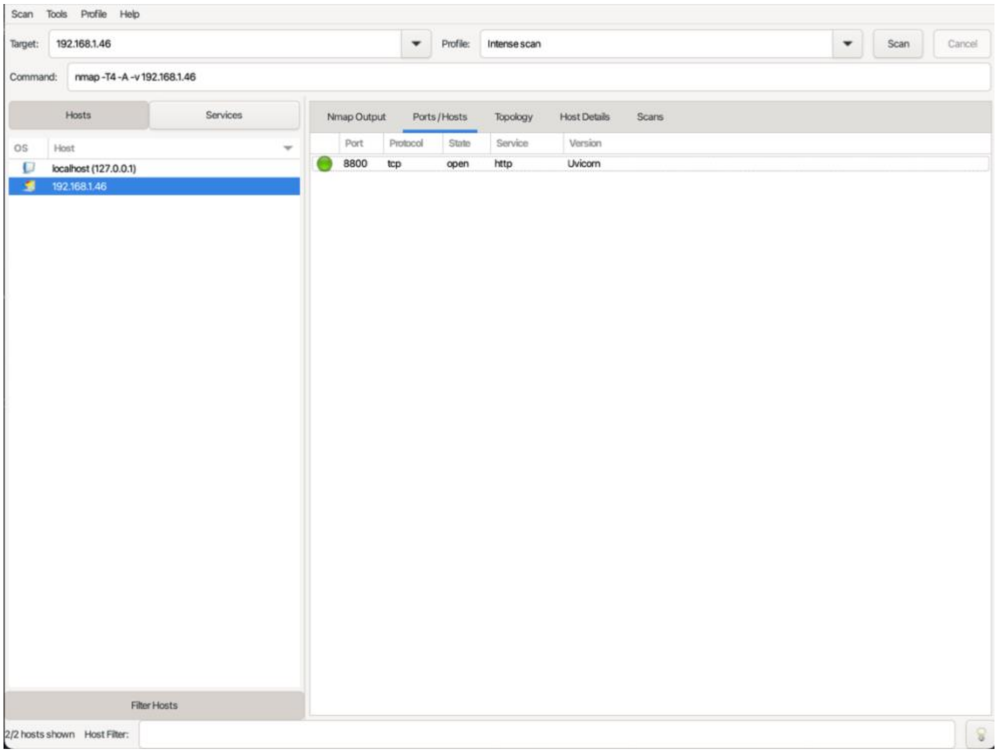
Command: nmap -T4 -A -v localhost

OS	Host
	localhost (127.0.0
	192.168.1.48

	Port	Protocol	State	Service	Version
●	88	tcp	open	kerberos-sec	Heimdal Kerberos (server time: 2025-09-08 15:05:44Z)
●	445	tcp	open	tcpwrapped	
●	5900	tcp	open	vnc	Apple remote desktop vnc

Attacker Notebook

Looks suspicious at first, but no. Because 88(Kerberos), 445 (File Sharing), and 5900(VNC) are normal for Macbook.



Target: 192.168.1.46

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.46

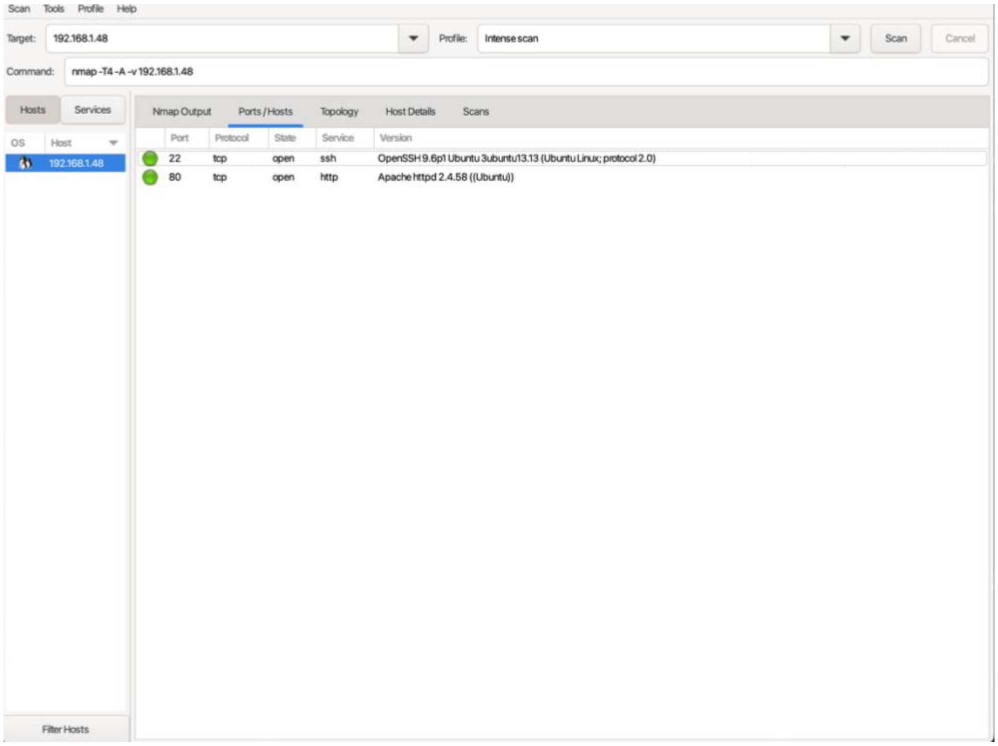
OS	Host
	localhost (127.0.0.1)
	192.168.1.46

	Port	Protocol	State	Service	Version
●	8800	tcp	open	http	Uvicorn

2/2 hosts shown Host Filter:

Target Notebook

Not suspicious, 8800 is expected because the target notebook is running Uvicorn on port 8800.



Target: 192.168.1.48

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.48

OS	Host
	192.168.1.48

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
●	80	tcp	open	http	Apache httpd 2.4.58 ((Ubuntu))

Target VM

Not suspicious. Port 22 and 80 are SSH and TCP, which are normal.

Q2.

Look at the information provided by nmap about your OS's on all 3 devices. Is the information correct? Why is it or why is it not correct?

Nmap's OS information is not fully correct across the 3 devices because:

- OS fingerprinting relies on network stack quirks (TCP/IP responses), which can be very similar across different Unix-like systems.
- Firewalls and virtualization distort or block the probes Nmap uses.
- Service banners ≠ OS (just because it sees Kerberos/SMB/VNC doesn't mean it knows it's macOS).

So while the open port detection is accurate, the OS guesses are only approximate and may be misleading.

Q3.

What do you think about the information you can get using nmap? Scary?

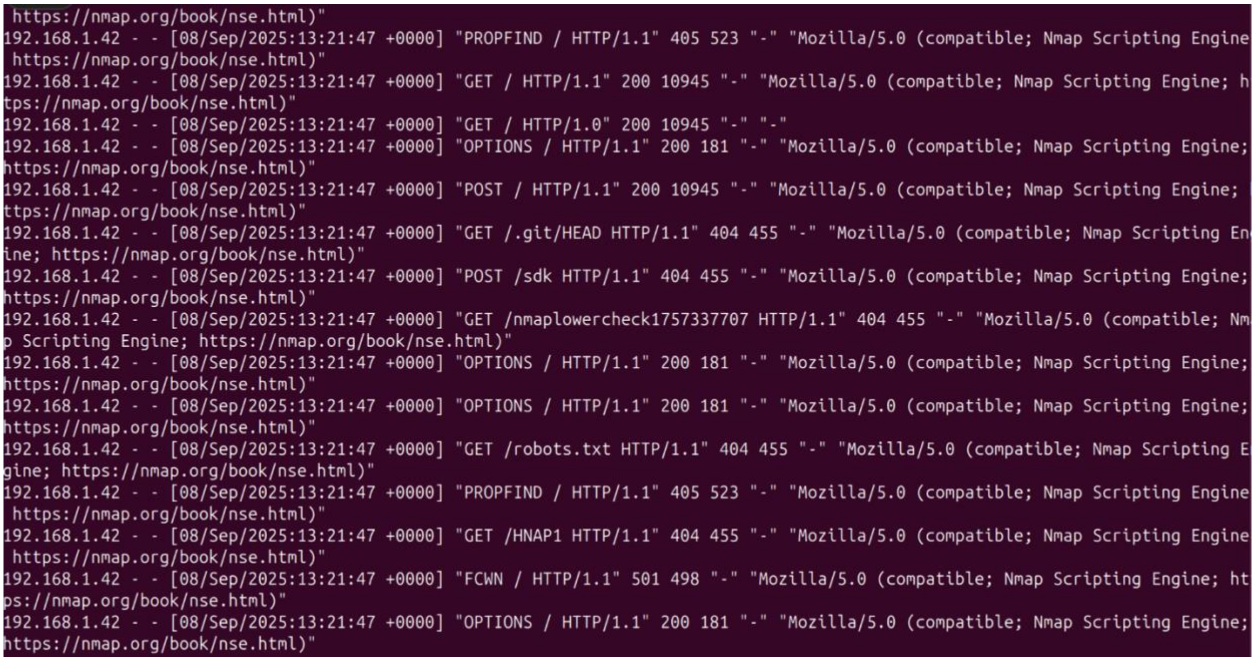
Yes, it is actually scary. With just a single command, Nmap can show

- open ports
- running services
- guess the operating system of a device

Now I understand the importance of closing unused ports and using strong firewalls.

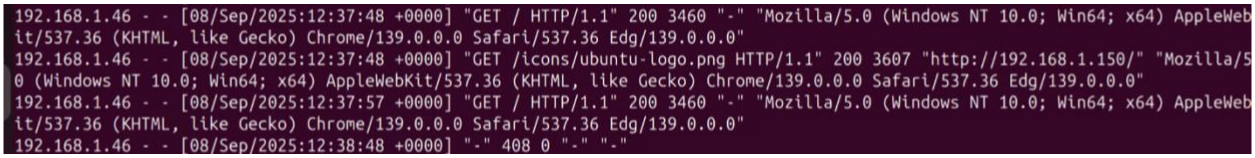
Q4.

Look at the access.log file for the web server in your Linux VM. What IP addresses do you see accessing the web server? Which devices do these IP addresses belong to?



```
 https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; h
tps://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
ttps://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "GET /.git/HEAD HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting En
ine; https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "GET /nmaplowercheck1757337707 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nm
p Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "GET /robots.txt HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting E
gine; https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "GET /HNAP1 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "FCWN / HTTP/1.1" 501 498 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; ht
ps://nmap.org/book/nse.html)"
192.168.1.42 - - [08/Sep/2025:13:21:47 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
```

192.168.1.42 Target Laptop Host IP



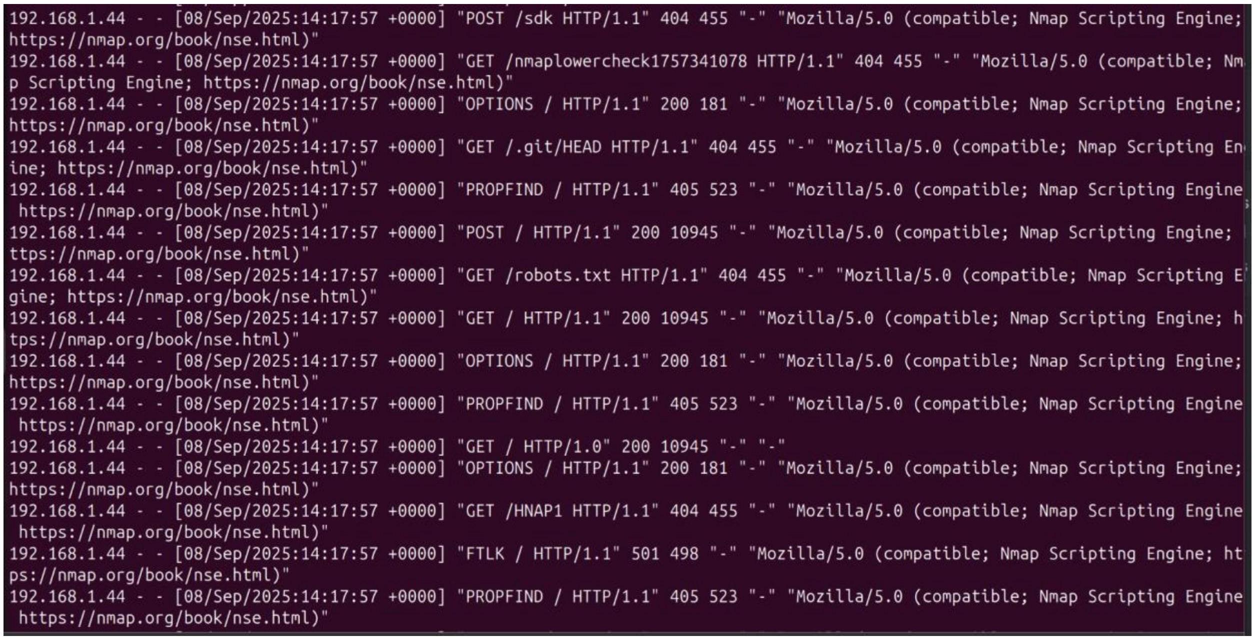
```
192.168.1.46 - - [08/Sep/2025:12:37:48 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
it/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36 Edg/139.0.0.0"
192.168.1.46 - - [08/Sep/2025:12:37:48 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.1.150/" "Mozilla/5
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36 Edg/139.0.0.0"
192.168.1.46 - - [08/Sep/2025:12:37:57 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
it/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36 Edg/139.0.0.0"
192.168.1.46 - - [08/Sep/2025:12:38:48 +0000] "-" 408 0 "-" "-"
```

192.168.1.46 Attacker Laptop Host IP

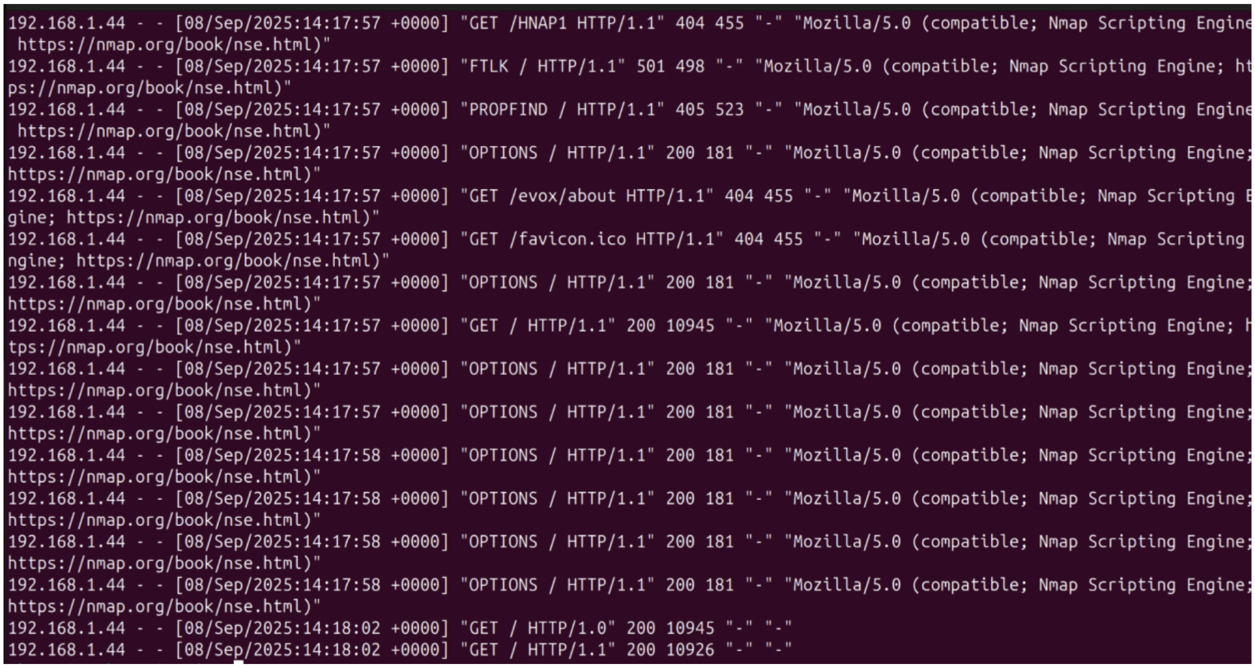
192.168.1.150 Target VM Host IP

Q5.

Find the nmap scan in the web server log. Copy the lines from the log file that were created because of the nmap scan.



```
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET /nmaplowercheck1757341078 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nm
p Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET /.git/HEAD HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting En
ine; https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
ttps://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET /robots.txt HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting E
gine; https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; h
tps://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET /HNAP1 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "FTLK / HTTP/1.1" 501 498 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; ht
ps://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
```

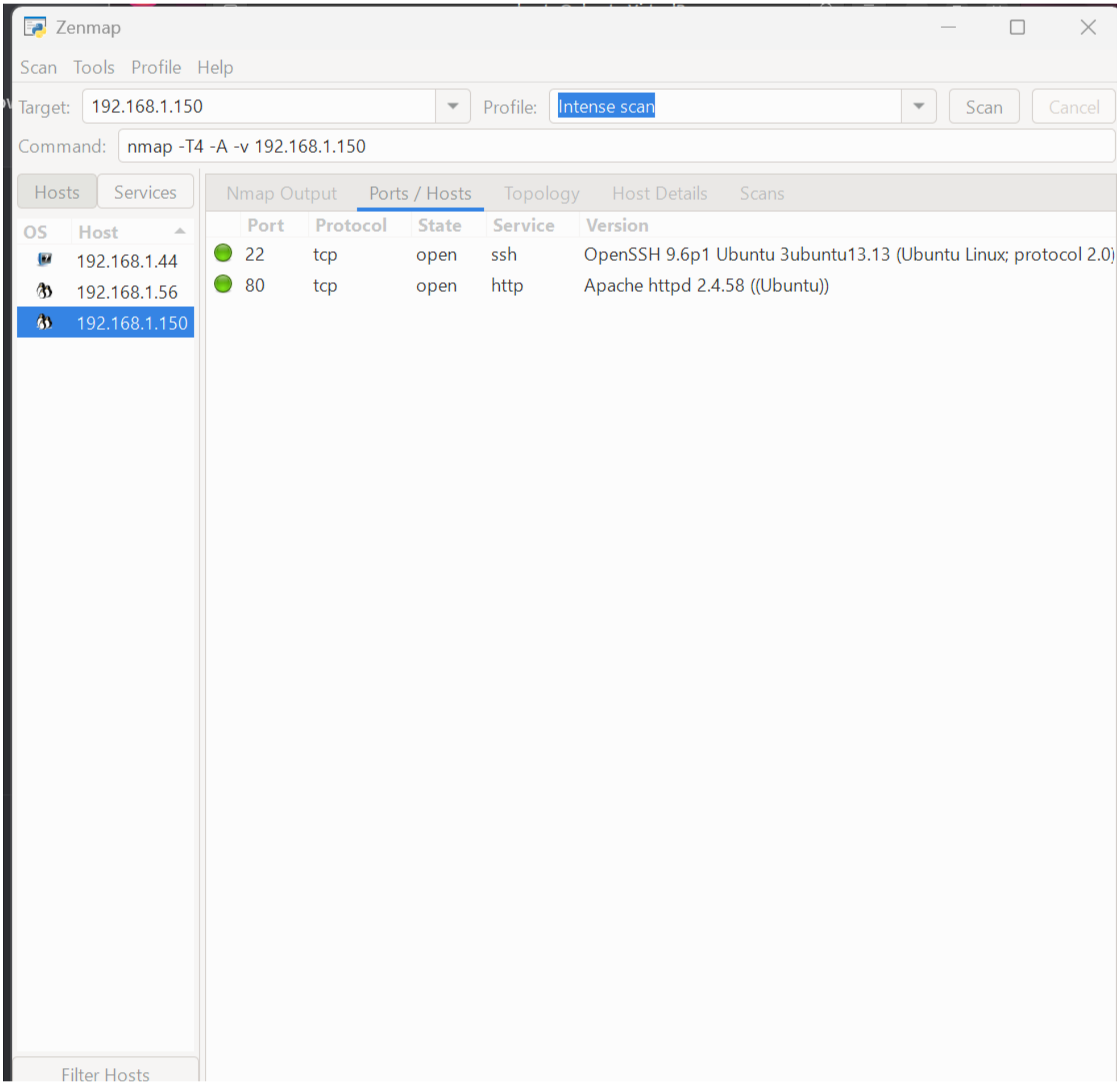


```
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET /HNAP1 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "FTLK / HTTP/1.1" 501 498 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; ht
ps://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "PROPFIND / HTTP/1.1" 405 523 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine
 https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET /evox/about HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting E
gine; https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET /favicon.ico HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting
ngine; https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; h
tps://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:57 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:58 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:58 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:58 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:17:58 +0000] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.1.44 - - [08/Sep/2025:14:18:02 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.1.44 - - [08/Sep/2025:14:18:02 +0000] "GET / HTTP/1.1" 200 10926 "-" "-"
```

Q6.

After you successfully install your iptable rule(s), how do the reported results from your new nmap scan compare to your previous scan before using iptables? Look to see if OS detection, port open results, etc. have changed. Something(s) have definitely changed.

Chayanin Kongsareekul 6532035021



Target: 192.168.1.150

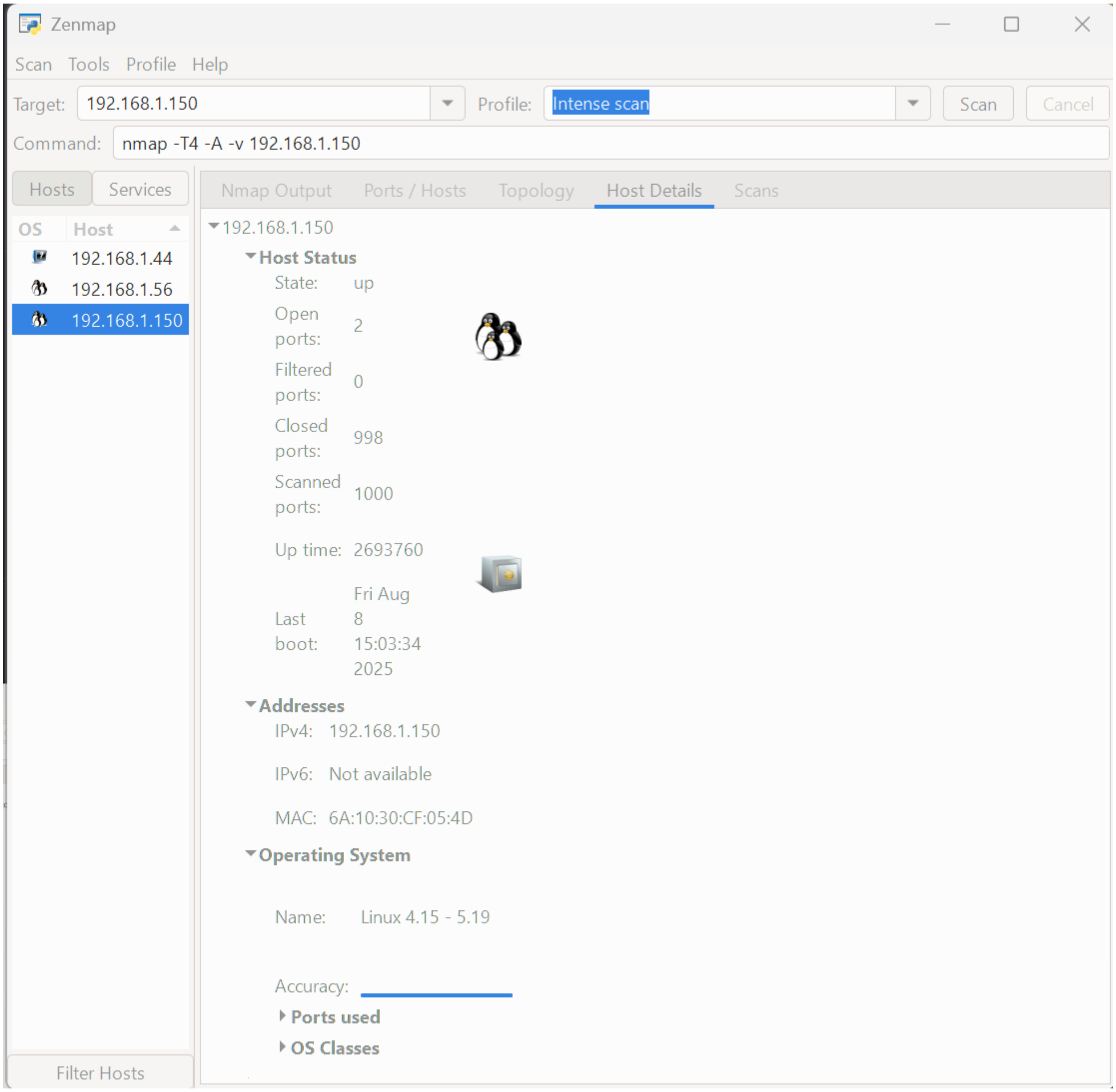
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.150

OS	Host
	192.168.1.44
	192.168.1.56
	192.168.1.150

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
●	80	tcp	open	http	Apache httpd 2.4.58 ((Ubuntu))

Before (1)



Target: 192.168.1.150

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.150

192.168.1.44
192.168.1.56
192.168.1.150

192.168.1.150

Host Status

State: up

Open ports: 2

Filtered ports: 0

Closed ports: 998

Scanned ports: 1000

Up time: 2693760

Last boot: Fri Aug 8 15:03:34 2025

Addresses

IPv4: 192.168.1.150

IPv6: Not available

MAC: 6A:10:30:CF:05:4D

Operating System

Name: Linux 4.15 - 5.19

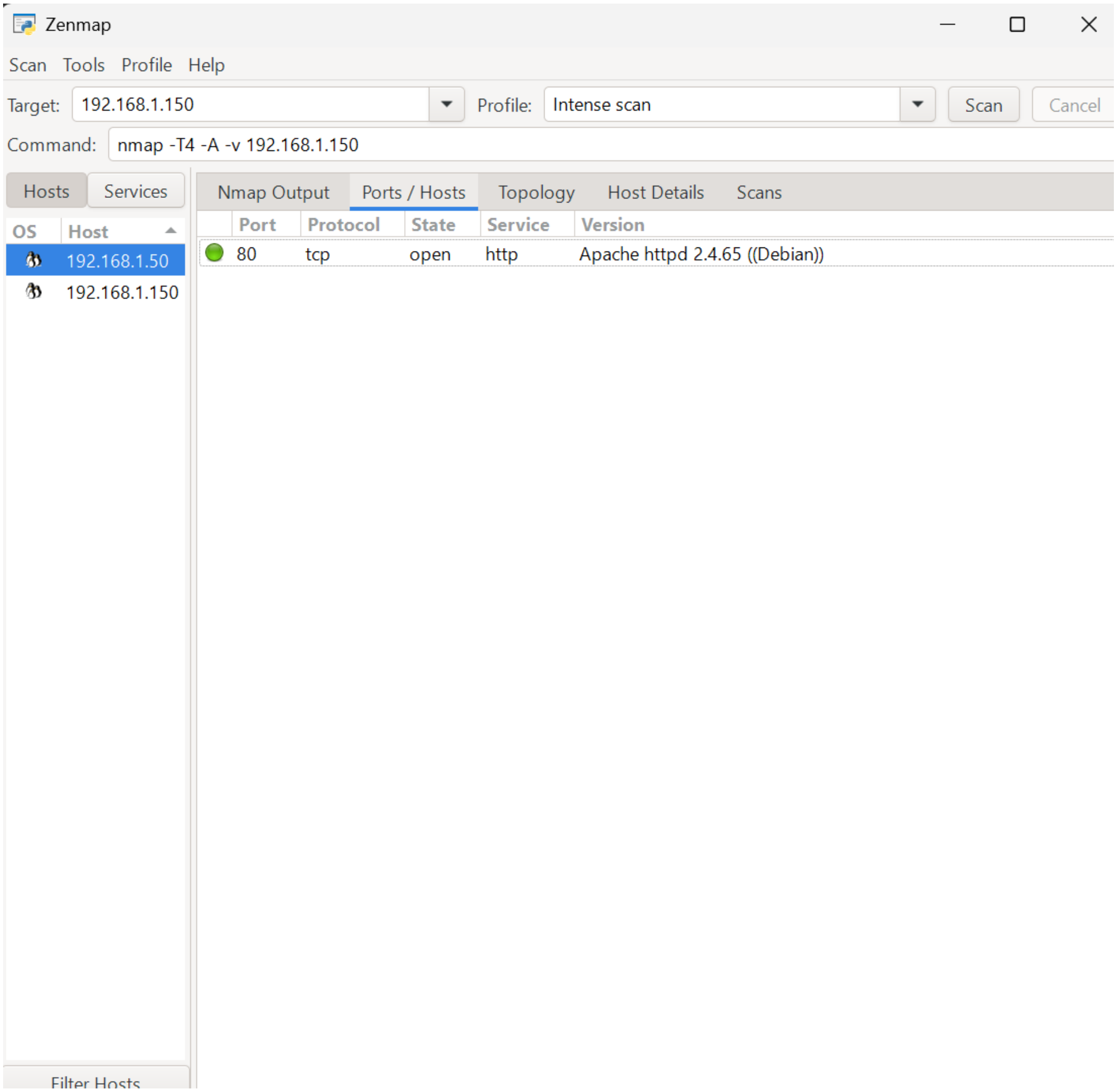
Accuracy:

Ports used

OS Classes

Before (2)

Chayanin Kongsareekul 6532035021



Target: 192.168.1.150

Profile: Intense scan

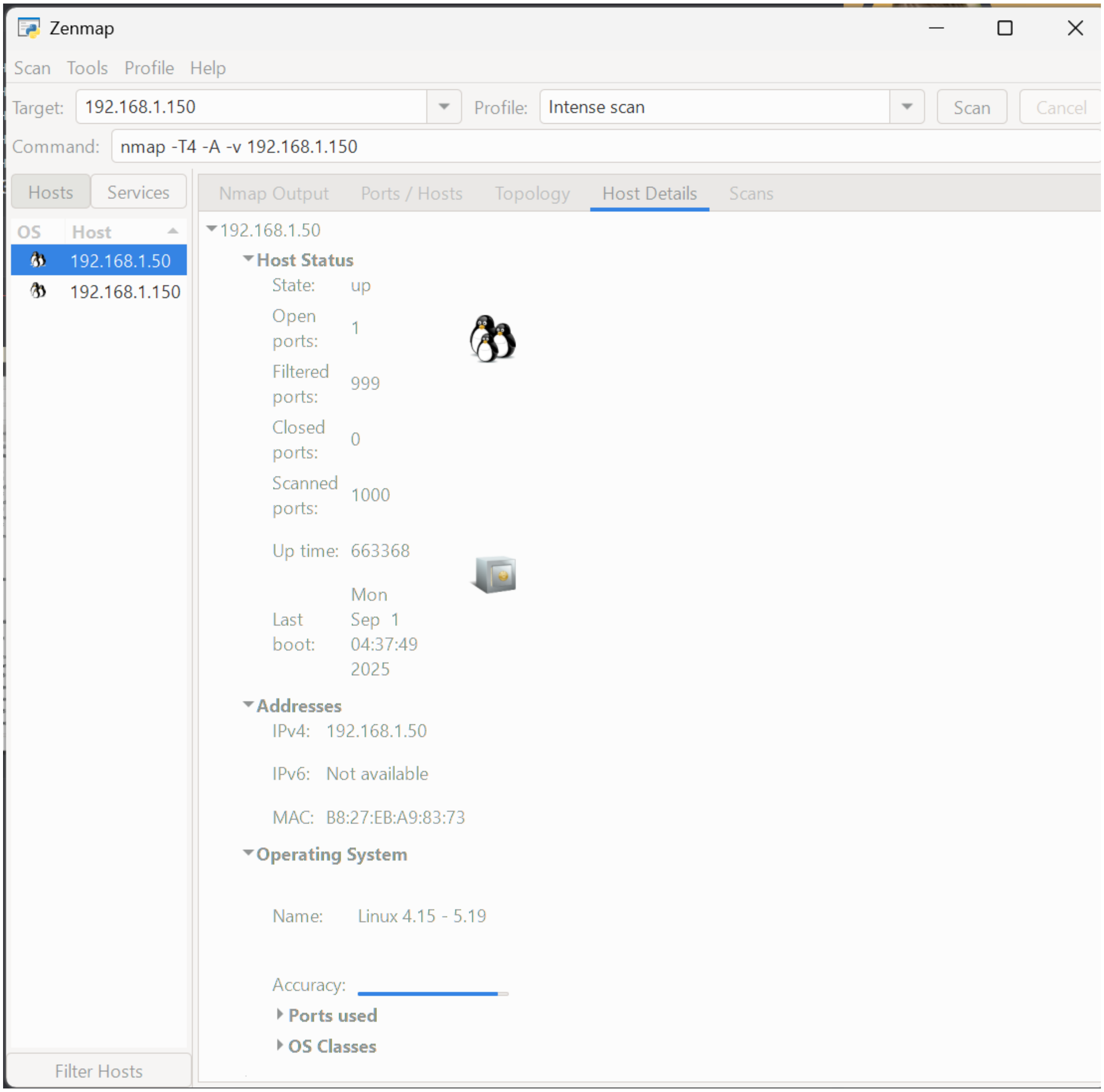
Command: nmap -T4 -A -v 192.168.1.150

OS	Host
	192.168.1.50
	192.168.1.150

	Port	Protocol	State	Service	Version
●	80	tcp	open	http	Apache httpd 2.4.65 ((Debian))

Chayanin Kongsareekul 6532035021

After (1)



Target: 192.168.1.150

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.150

192.168.1.50

Host Status

State: up

Open ports: 1

Filtered ports: 999

Closed ports: 0

Scanned ports: 1000

Up time: 663368

Last boot: Mon Sep 1 04:37:49 2025

Addresses

IPv4: 192.168.1.50

IPv6: Not available

MAC: B8:27:EB:A9:83:73

Operating System

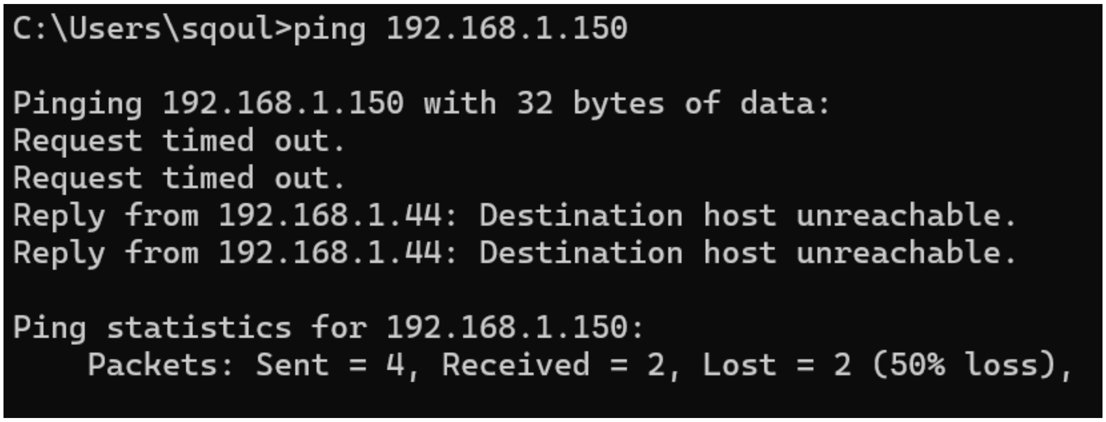
Name: Linux 4.15 - 5.19

Accuracy:

Ports used

OS Classes

After (2)



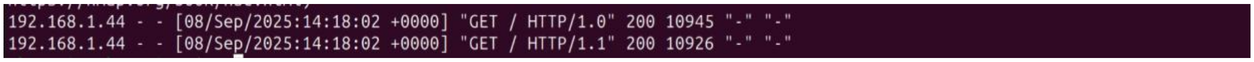
```
C:\Users\sqoul>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.1.44: Destination host unreachable.
Reply from 192.168.1.44: Destination host unreachable.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
```

After (3)

- NMAP only show PORT 80, PORT 22 missing.
- Closed port became filtered port.
- Can’t Ping.

Q7.

Notice that nmap can still figure out you have Apache httpd running. Look at the access.log file for the web server in your Linux VM. Are the logs the same as in Part II?



```
192.168.1.44 - - [08/Sep/2025:14:18:02 +0000] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.1.44 - - [08/Sep/2025:14:18:02 +0000] "GET / HTTP/1.1" 200 10926 "-" "-"
```

Log

Yes, logs are the same.

Q8.

Explain whether or not you could prevent nmap from reaching the web server while still allowing legitimate clients to get service. Will a firewall be sufficient for this? Or do you need some other device? Please think critically about this.

Can a firewall alone stop nmap but allow real clients?

- **No.** A firewall can block unused ports, but if port 80/443 is open, nmap traffic looks like normal web traffic.
- Scanners can be stealthy (slow scans, fragmented packets, distributed sources).
- Firewall rules can't reliably tell "scanner" from "browser."

What a firewall can do

- Allow only required ports (deny everything else).
- Rate-limit connections and block obvious scan patterns.

What's needed beyond a firewall

- VPN / client IP allowlisting → only trusted clients can connect.
- Mutual TLS (client certs) → server only accepts authenticated clients.
- Reverse proxy / CDN / WAF → hides the real server, filters malicious traffic.

Q9.

What are your firewall rules? Run iptables -L on your VM and enter the output

here.

```
Chain INPUT (policy DROP 2425 packets, 1209K bytes)
 pkts bytes target     prot opt in     out     source               destination

    9  1873 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0

  415 40409 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            ctstate
RELATED,ESTABLISHED

   67  3660 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80

    0     0 ACCEPT     6    --  *      *       192.168.1.42         0.0.0.0/0            tcp dpt:22

   16  2608 DROP       1    --  *      *       0.0.0.0/0            0.0.0.0/0

    2   104 ACCEPT     6    --  *      *       192.168.1.44         0.0.0.0/0            tcp dpt:22
```

```
Chain FORWARD (policy DROP 0 packets, 0 bytes)

 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 565 packets, 188K bytes)

 pkts bytes target     prot opt in     out     source               destination
```